

### REMARKS

Claims 1, 8, 12, 14, 16, 18, 20, 27, 30, 31 and 34 have been amended.

Claims 1 – 36 are present in the subject application.

In the Office Action, the Examiner has rejected claims 1 – 10, 12 – 14, 16 – 18, 20 – 29 and 31 – 36 under 35 U.S.C. §102(e) and has rejected claims 11, 15, 19 and 30 under 35 U.S.C. §103(a). Reconsideration of the subject application is respectfully requested in view of the following remarks.

The Examiner has rejected claims 1 – 10, 12 – 14, 16 – 18, 20 – 29 and 31 – 36 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,510,415 (Talmor et al.). Briefly, the present invention is directed toward a system for facilitating secure network communications including a security computer system and corresponding software. The security system is utilized in conjunction with a voice browser residing on a server system. A user accesses the network by placing a call to the voice browser system. The voice browser includes a software module that creates a secure connection to the security system. The user provides an identification to the voice browser system that is transferred to and verified by the security system. Once the identification is verified, the user is prompted by the voice browser system to speak a phrase for voice verification. The verification speech signals are transferred from the voice browser system to the security system to verify those speech signals against speech signals of a particular authorized user associated with the identification and stored in a database. When the user is verified, the security system retrieves a user private key and certificate from the database. In response to the user subsequently accessing a web site residing on a secure server, the secure server and voice browser system initiate a secure key exchange. During the key exchange, data packets containing security information are transferred from the voice browser system to the

security system for processing, while security information from the security system is transferred to the secure server via the voice browser system. The resulting session key is securely transferred to the voice browser system to facilitate secure communications between the voice browser system and secure server.

In other words, the present invention basically provides a system to negotiate and handle secure communications for the voice browser. Since the voice browser does not store user information enabling secure communications (e.g., user keys and certificates) with a secure network site, security information received by the voice browser from an accessed secure network site is identified and processed by the present invention to facilitate secure communication between the voice browser and secure site. In addition, authorized users are verified by the present invention based on voice signals in order to retrieve the user information (e.g., keys and certificates) enabling the secure communications which is stored remote from the voice browser.

This rejection is respectfully traversed since the Talmor et al. patent does not disclose, teach or suggest a voice responsive network interface and negotiation of communication parameters with a secure network site for the network interface to facilitate secure communications over a network between that site and the network interface as recited in the claims. However, in order to expedite prosecution of the subject application, independent claims 1, 12, 16, 20, 31 and 34 have been amended to further clarify these features. In particular, independent claims 1, 12, 16 and 20 recite the features of: identifying security related information received by the network interface from a secure network site in response to the network interface accessing the secure network site based on voice commands from the user; storing remote from the network interface voice and security information associated with

authorized users; retrieving the security information of a verified user stored remote from the network interface; and negotiating communication parameters with the secure network site utilizing retrieved security information in response to receiving the identified security information to facilitate secure communications over the network between the secure site and the network interface. Independent claims 31 and 34 similarly recite retrieving remotely stored security information of a verified user and negotiating communication parameters with a secure network site utilizing the retrieved security information to facilitate secure communications over the network between the secure site and the network interface in response to the network interface accessing the secure network site based on voice commands from the user.

The Talmor et al. patent does not disclose, teach or suggest these features. Rather, the Talmor et al. patent is directed toward a system for authorizing user access to a secure site including a memory unit, first and second input devices, and first and second processing devices. The memory unit stores voice prints and identities of the set of individuals that have access to the secure site. The first input device is for inputting information that identifies the user as a member of the set. The second input device is for inputting temporary user voice data. The first processing device is for generating a temporary voice print from the temporary data. The second processing device is for comparing the temporary voice print to the stored voice prints. Access is granted only if the temporary voice print is most similar to the voice print of the individual that the user claims to be (e.g., See Abstract).

In an embodiment accessing a Web site, a user operating a client enters a Web page stored on a Web server and initiates user authentication by activating an authentication button. An authentication server receives from an E-commerce server (in communication or integrated with the Web server) ID request data (i.e., including an authentication request number, a Web

server identifier, user provided voice data (for authentication) and hardware and software keys) and processes the data to authenticate the user by voice. The authentication results are returned to the Web server for display on the Web page (e.g., See Column 13, line 65 to Column 14, line 16).

Thus, the Talmor et al. patent simply discloses a system that grants access to a site (e.g., Web site) in accordance with authentication of a user based on voice signals and is generally silent with respect to the manner in which communications are conducted between the servers and client. There is no disclosure, teaching or suggestion of a voice responsive interface and negotiation of communication parameters utilizing security information of a verified user remotely stored from the network interface for secure communications over the network between the voice responsive interface and secure site as recited in each of the independent claims. In fact, the Talmor et al. patent discloses conventional access of the Web page by a user client with authentication preferably initiated by a button or mouse click (due to the presence of a click counter), where the authentication server does not engage in negotiation of security parameters between the servers and client, but rather merely authenticates the user provided voice data and sends results back to the Web server for display on the Web page.

Since the Talmor et al. patent does not disclose, teach or suggest the features recited in independent claims 1, 12, 16, 20, 31 and 34 as discussed above, these claims are considered to be in condition for allowance.

Dependent claims 2 – 10, 13 – 14, 17 – 18, 21 – 29, 32 – 33 and 35 – 36 depend either directly or indirectly from independent claims 1, 12, 16, 20, 31 or 34, and, therefore, include all the limitations of their parent claims. Dependent claims 8, 14, 18 and 27 have been amended for consistency with their amended parent claims. The dependent claims are considered to be in

condition for allowance for substantially the same reasons as discussed above in relation to their parent claims and for further limitations recited in these claims.

The Examiner has rejected claims 11, 15, 19 and 30 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,510,415 (Talmor et al.) in view of U.S. Patent No. 6,671,672 (Heck). Briefly, the present invention is directed toward a system for facilitating secure network communications as described above. The Examiner takes the position that the Talmor et al. patent discloses the invention as substantially claimed, except for the feature of an enrollment module. The Examiner further alleges that the Heck patent teaches this feature and that it would have been obvious to combine the teachings of the Talmor et al. and Heck patents to attain the claimed invention.

This rejection is respectfully traversed. Initially, claims 11, 15, 19 and 30 depend either directly or indirectly from independent claims 1, 12, 16 and 20 and, therefore, include all the limitations of their parent claims. Claim 30 has been amended for consistency with its amended parent claim. As discussed above, the Talmor et al. patent does not disclose, teach or suggest the features recited in independent claims 1, 12, 16 and 20 of a voice responsive network interface and negotiating communication parameters for the network interface utilizing retrieved security information of a verified user to facilitate secure communications between the secure network site and the network interface. The Heck patent does not compensate for the deficiencies of the Talmor et al. patent and similarly does not disclose, teach or suggest these features. Rather, the Heck patent is directed toward a voice authentication system having a cognitive recall mechanism for password verification. A user is enrolled for password verification by receiving a first voice input from the user representing the password prompt and a second voice input representing a correct response to the password prompt. The first and second voice inputs may

be stored as waveforms, as voiceprints, recognized speech data, or a combination thereof. During verification, the identity of the user is verified by outputting the user-provided password prompt and evaluating a response to the password prompt against the correct response. Thus, the user is able to select his own password prompt to facilitate cognitive recall of the password during a subsequent verification phase (e.g., See Abstract).

The Heck system includes a computer system with a voice-activated software application functionally coupled to authentication software. The voice-activated software application may enable bank customers or investors to perform transactions by voice over a telephone (See Column 3, lines 1 - 30). Thus, the Heck patent simply discloses a manner of authenticating a user based on voice signals and a spoken password prior to permitting a transaction. There is no disclosure, teaching or suggestion of a voice responsive network interface to access network sites by user voice commands and negotiation of communication parameters utilizing security information of a verified user remotely stored from the network interface for secure communications over the network between the voice responsive interface and secure site as recited in the claims.

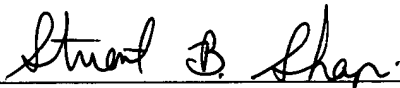
Since the Talmor et al. and Heck patents, either alone or in combination, do not disclose, teach or suggest the features recited in claims 11, 15, 19 and 30 as discussed above, these claims are considered to be in condition for allowance.

In addition to the foregoing, there is no motivation or suggestion to combine the teachings of the Talmor et al. and Heck patents. As discussed above, the Talmor et al. patent is directed toward a manner of authenticating a user based on a particular comparison of voice signals to permit entry to a site (e.g., Web site). The Heck patent is directed toward

authenticating a user by voice authentication and a spoken password to enable a transaction. Thus, the patents are directed toward diverging applications and there is no apparent reason, suggestion or motivation to combine their teachings. Accordingly, the proposed combination of the Talmor et al. and Heck patents does not render the claimed invention obvious.

The application, having been shown to overcome issues raised in the Office Action, is considered to be in condition for allowance and a Notice of Allowance is earnestly solicited.

Respectfully submitted,

  
\_\_\_\_\_  
Stuart B. Shapiro  
Registration No. 40,169

EDELL, SHAPIRO & FINNAN, LLC  
1901 Research Boulevard, Suite 400  
Rockville, Maryland 20850-3164  
(301) 424-3640

Hand Delivered: 10/26/04